APPENDIX:

The Appendix includes the following items:

- 5 pages of background,

- 22 pages of discussion, and

- 4 pages of a table comparing the present invention to the applied reference.

M tivation starting at page 3 "Claim Rejecti ns – 35 USC §102" and ending at page 7 before "Claim Rejecti ns – 35 USC § 103 f the Office Acti n Summary as of 11/21/2003

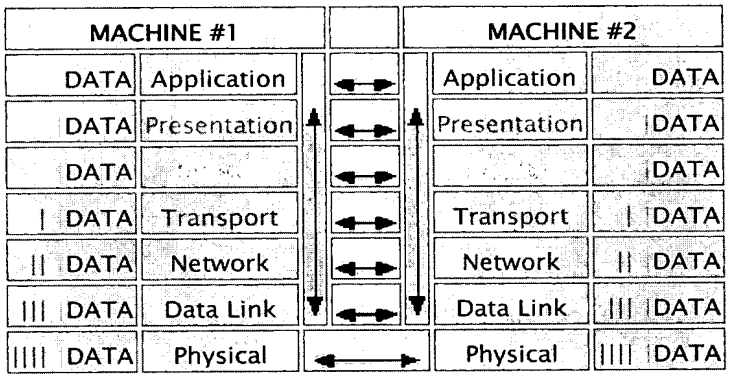
To make things as clear as possible the Open Standards Interconnect (OSI) model developed by the International Standards Organization (ISO) is important to use as a reference. For that purpose this document is written.

The OSI model is also recognized by Green.

This paper gives a brief description of the topics OSI, TCP / IP and Firewall.

The International Standards Organization (ISO) developed a theoretical model of how networks should behave and how they are put together. The Open Standards Interconnect (OSI) model is used through the industry today to describe various networking issues. One can use it as a point of reference to learn how various technologies interact, where they reside, what functions they perform and how each protocol communicates with other protocols.

The OSI model has seven layers:



A few basic concepts can be gleaned from the multi-colored diagram above.

1. Network-capable Applications produce DATA.
2. Each protocol layer adds a header to the data it receives from the layer above it. This is called 'encapsulation'. Encapsulated data is transmitted in Protocol Data Units (PDUs). There are Presentation PDU's, Session PDU's, Transport PDU's etc.
3. PDU's are passed down through the stack of layers (called 'the stack' for short) until they can be transmitted over the Physical layer.
4. Any layer on one machine speaks the same language as the same layer on any other machine, and therefore can communicate via the Physical layer (this communication is represented by the ◄►symbols).
5. Data passed upwards is unencapsulated before being passed further up (colored bars).
6. All information is passed down through all layers until it reaches the Physical layer (represented by the vertical red arrows).
7. The Physical layer chops up the PDU's and transmits the PDU's over the wire. The Physical layer provides the real physical connectivity between machines over which all communication occurs (represented by ◄——►).

Data from one layer is supposed to be passed down into the layer below it. In the 'real world', the process of encapsulation (adding a header) doesn't always occur at all layers.

Data passed over the Internet gets the first header from the application, then from Transport Control Protocol (TCP), then Internet Protocol (IP) puts in a header and passes it down. After that point, it's all hardware. Although IP doesn't conform completely to the model above, the model is still a good reference point for discussing network technologies and protocols.

PHYSICAL LAYER

The Physical layer provides for physical connectivity between networked devices. Transmission and receipt of data from the physical medium is managed at this layer.

The Physical layer receives data from the Data Link Layer, and transmits it to the wire. The Physical layer controls frequency, amplitude, phase and modulation of the signal used for transmitting data, and performs demodulation and decoding upon receipt.

Note that for two devices to communicate, they must be connected to the same type of physical medium (wiring). Ether to Ether, FDDI to FDDI etc. Two end stations using different protocols can only communicate through a multi-protocol bridge or a router.

The physical layer is responsible for two jobs:

1. Communication with the Datalink layer.
2. Transmission and receipt of data.

DATA LINK LAYER

The Datalink Layer is the second layer of the OSI model. The datalink layer performs various functions depending upon the hardware protocol used, but has four primary functions:

1. COMMUNICATION with the Network layer above.
2. SEGMENTATION of upper layer datagrams (also called packets) into frames in sizes that can be handled by the communications hardware.
3. BIT ORDERING. Organizing the pattern of data bits before transmission (packet formatting)
4. COMMUNICATION with the Physical layer below.

This layer provides reliable transit of data across a physical link. The datalink layer is concerned with physical addressing, network topology, physical link management, error notification, ordered delivery of frames, and flow control.

NETWORK LAYER

Internet Protocol (IP), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP) all function at the Network layer. Outbound data is passed down from the Transport layer, is encapsulated in the Network layer's protocol and then sent to the Datalink layer for segmentation and transmission.

Inbound data is de-fragmented in the correct order, the IP headers are removed and then the assembled datagram is passed to the Transport layer.

The Network layer is concerned with the following primary functions:

1. Communication with the Transport layer above.
2. Management of connectivity and routing between hosts or networks.
3. Communication with the Datalink layer below.

TRANSPORT LAYER

It is the transport layer's responsibility to see to the detection of errors, and retransmission of data to recover those errors or lost data. The Transport layer may use a variety of techniques such as a Cyclic Redundancy Check, windowing and acknowledgements. If data is lost or damaged it is the Transport layer's responsibility to recover from that error.

1. Communicate with the Session layer above.
2. Detect errors and lost data, retransmit data, reassemble datagrams into datastreams
3. Communicate with the Network layer below.

SESSION LAYER

The session layer tracks connections, also called 'sessions'. E.g. The session layer should keep track of multiple file downloads requested by a particular FTP application, or multiple telnet connections from a single terminal client, or web page retrievals from a Web server. In the World of TCP/IP this is handled by application software addressing a connection to a remote machine and using a different local port number for each connection.

The session performs the following functions:

1. Communication with the Presentation layer above.
2. Organize and manage one or more connections per application, between hosts.
3. Communication with the Transport layer below.

PRESENTATION LAYER

The Presentation layer handles the conversion of data formats so that machines can 'present' data created on other systems. The presentation layer would handle the conversion of data in JPG/JPEG format to Sun Raster format so that a Sun machine can display a JPG/JPEG image.

The Presentation layer performs the following functions:

- Communication with the Application layer above.
- Translation of standard data formats to formats understood by the local machine.
- Communication with the Session layer below.

APPLICATION LAYER

The application layer is the application in use by the user. This could be a web browser, an FTP, IRC, Telnet client other TCP/IP based application like the network version of Doom, Quake, or Unreal.
The Application layer provides the user interface, and is responsible for displaying data and images to the user in a recognizable format. The application layers job is to organize and display data in a human compatible format, and to interface with the Presentation layer.

TCP / IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "stateless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone or fax conversations that require a dedicated connection for the call duration). Being stateless frees network paths so that everyone can use them continuously. (Note that the TCP layer itself is not stateless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.)

Protocols related to TCP/IP include the User Datagram Protocol (UDP), which is used instead of TCP for special purposes. Other protocols are used by network host computers for exchanging router information. These include the Internet Control Message Protocol (ICMP), the Interior Gateway Protocol (IGP), the Exterior Gateway Protocol (EGP), and the Border Gateway Protocol (BGP).

FIREWALL

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination.

A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

REMARK APPLICANT

The used word "connection" in the GREEN patent might be interpreted as follows:

A.

"Connection" is a synonym for "forwarding".

e.g.

To "close a connection" means that data is not forwarded to its destination.

B.

"Connection" means a "logical" communication session.

Motivati n starting at page 3 "Claim Rejecti ns – 35 USC §102" and nding at page 7 bef re "Claim Rejections – 35 USC § 103 f the Office Action Summary as of 11/21/2003

Open Standards Int rconn ct (OSI) m del

While reading this document important is to keep in mind the Open Standards Interconnect (OSI) model developed by the International Standards Organization (ISO). The OSI model is also recognized by Green.

Connection

Another important subject is the definition of the word "connection".

1)
In telecommunication and computing in general, a connection is the successful completion of necessary arrangements so that two or more parties (for example, people or programs) can communicate at a long distance. In this usage, the term has a strong physical (hardware) connotation.

A dialup (sometimes called a switched) connection is a telephonic arrangement that is set up only when needed, using shared, circuit-switched communication lines. A dedicated (sometimes called a non switched) connection is a continuous, always available connection (familiar to users of Digital Subscriber Line or DSL service). A leased line is a line rented from a telephone company that provides dedicated connection between two points (such as a headquarters office and a manufacturing plant).

2)
In computer programming, a connection is the setting up of resources (such as computer memory and buffers) so that a particular object such as a database or file can be read or written to.

Typically, a programmer encodes an OPEN or similar request to the operating system that ensures that system resources such as memory are set up, encodes READS and WRITES or similar requests, and then encodes a CLOSE when a connection is no longer needed so that the resources are returned to the system for other users.

A closely related term is session, which is sometime used to distinguish the ability to communicate for some duration in a logical sense. In this usage, the connection is regarded as the physical setup and the session is regarded as the logical setup. A session could be terminated and the connection maintained with the expectation of a new session later.

This document

How this document is build up.

1. The text of the examiner is divided up in parts.
2. When the examiner refers to the patent of GREEN also those text parts are brought into this document.
3. Where applicable comments of the applicant are written down.

Legend

Text = Words of the examiner
Text = Quoted text from GREEN 6,003,084
Text = Comment of applicant

EXAMINER

As per claim 1, Green teaches a method for protecting data communication, traffic between a first communication station (11) (see Fig.2, #216; and col.7, lines 60-62) and a second communication station (12) (see Fig.2, #214; and col.7, lines 60-62),...

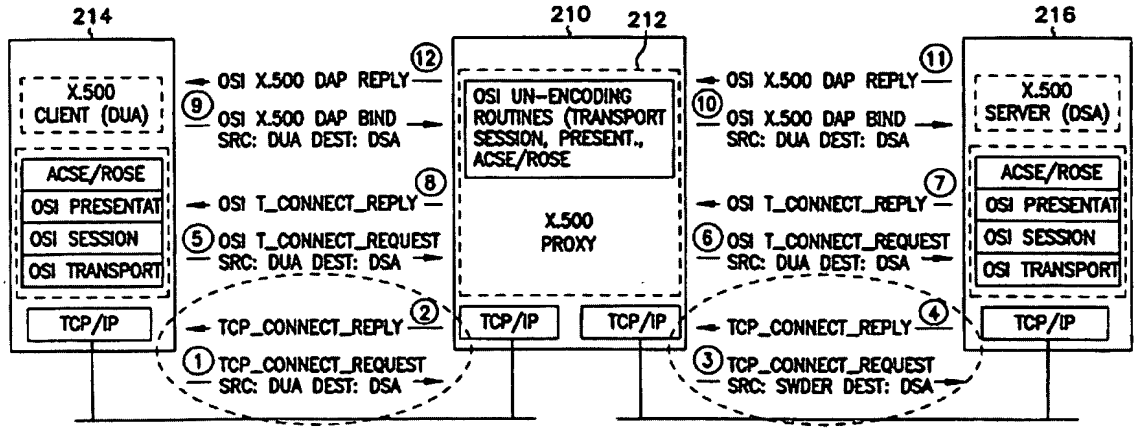


FIG. 2

GREEN col.7, lines 60-62

Also shown in FIG. 2 are a client 214 and server 216 for which connections and data transfers will be described further below.

COMMENT 1

RCID is developed to be used in a telecom environment.
This means that RCID complies with given standards of the International Telecommunications Union (ITU) which is a formal, worldwide telecommunications standards body.
The ITU is a charter organization of the United Nations (UN), and is based in Geneva, Switzerland.

When a connection is made there is one physical AND one logical connection between TWO communication stations in place.
When no communication is necessary there is no physical connection in place at all.

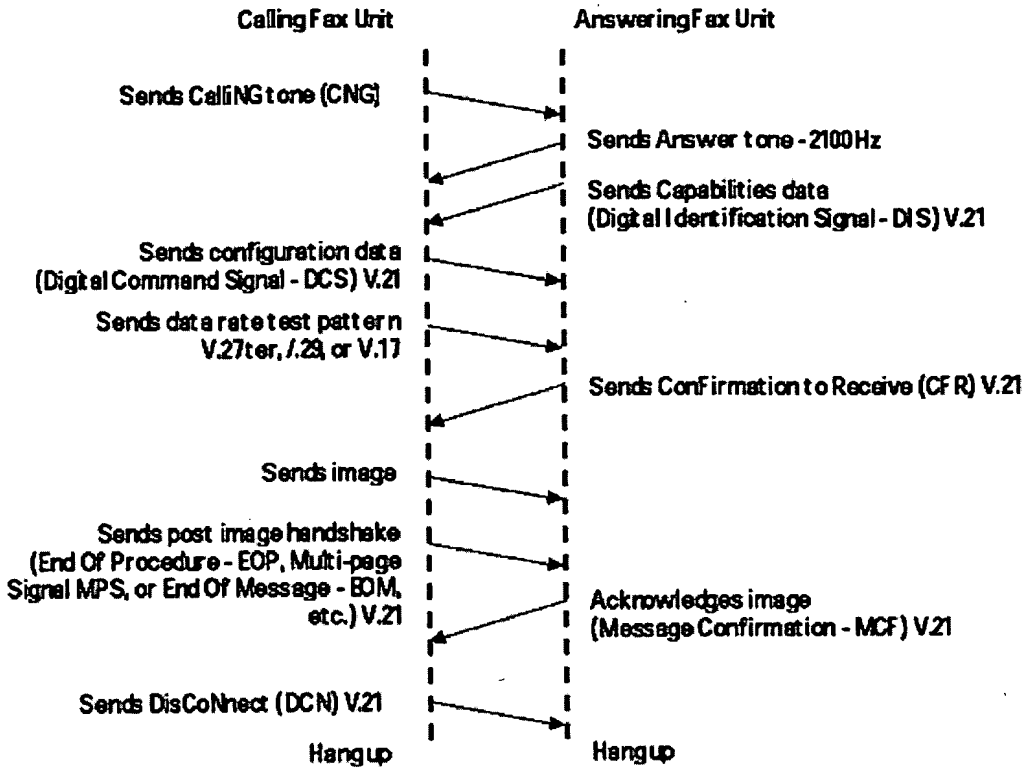


FIG. fax communications ITU standard

GREEN is typically developed to be used in a network environment.
When a connection is made there are always N+1 connections between N+1 communication stations.
Those connections are ALL physical.
There MIGHT be logical connections too (for instance one server with N clients, or N servers with N clients).

To close one connection physically will immediately result in serious consequences while ALL logical connections are closed too.

Such information security incidents are well known and not very much appreciated as this means that the corporate network IS DOWN.

Persons of ordinary skill in the art will NEVER close communication in a physical way, because this will result in the same damaged as when a security incident occurs like a successful Denial of Service (DoS) attack initiated by a hacker.

EXAMINER
...in which the data is dispatched according to a data protocol from the second communication station to the first communication station (see col.5, lines 29-32),...

GREEN col.5, lines 29-32
Protocol data units are interrogated for conformance to a protocol session, and optionally further decoded to add additional application specific filtering.

COMMENT 2
RCID only monitors one type of standardized ITU protocol at the time.
That protocol itself incorporates the message (for instance a fax message)

GREEN has to monitor much more and diverging protocols at the same time.
Each protocol may "carry" one or more messages (for instance different types of office applications information)

EXAMINER
...comprising the steps of:
(i) receiving the data from the second communication station (12) in a data communication protection device (10) (see col.7, lines 63-66 and col.8, lines 16-17),...

GREEN col.7, lines 63-66
The Sidewinder security system has special TCP/IP networking modifications which allow it to accept a TCP connection request even though the data was not addressed to it.

COMMENT 3
RCID does not have (there is no need) such a networking modification while RCID operates in a telecom environment.
Every physical and logical connection is made through RCID.
There are only two devices, one sender and one receiver, involved in the communication.

Sidewinder however has to deal, depending on the size of the network, with N+1 (physical) users.
According to the specs of Sidewinder now-a-days with a maximum capacity of 25 to 40.000+ users.
This means a total of concurrent (logical) CONNECTIONS between 500.000 and 1.000.000

To close a connection physically means that ALL logical connections are closed too.
The result of this is the same as the result of a positive Denial of Service attack (DoS) by a hacker.
Such information security incidents are well known and not very much appreciated as this means that the corporate network IS DOWN.

GREEN col.8, lines 16-17
A client transfers transport data or PDUs to a TCP stack in the program.

COMMENT 4
RCID does not need nor use those kinds of stacks while RCID is operating in a telecom environment.
Only two devices are communicating with each other at the time, using only one specific ITU standardized protocol.

EXAMINER
...the protection device having
i) a first input for connection to an incoming communication line receiving the data communication from the second communication station,
ii) a second input for connection to the first communication station (see Fig.2, and Fig.3b),...
iii) a comparison and forwarding module connected intermediate the first input and the second input and establishing a physical communication link between the first input and the second input (see Fig.2, #212 and col.7, lines 57-60),...

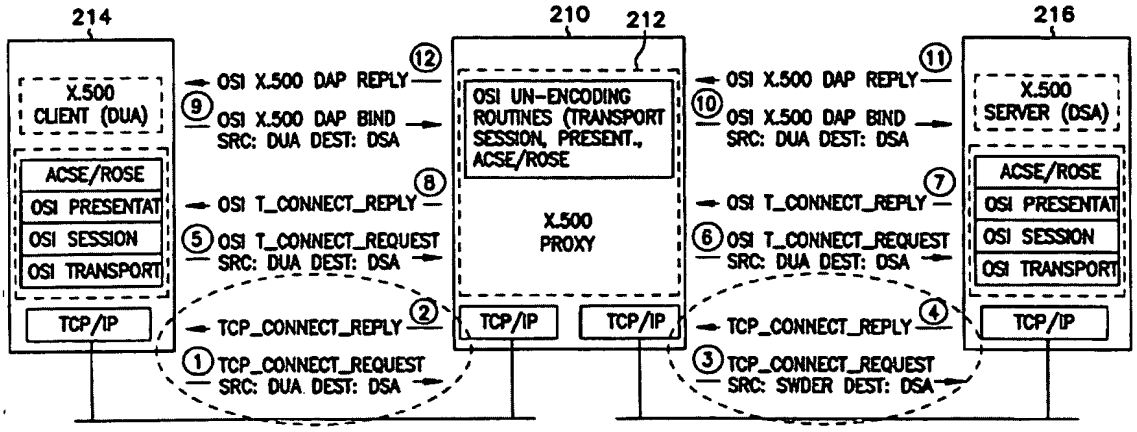


FIG. 2

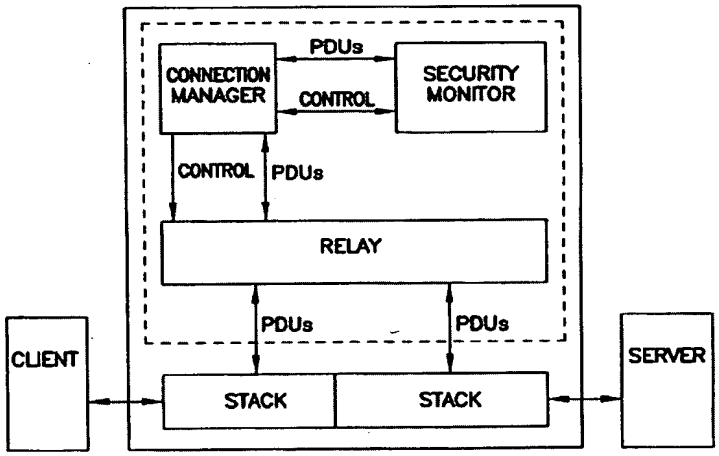


FIG. 3b

GREEN col.7, lines 57-60

Computer program 210 further comprises a proxy 212 which is used to process communications complying with different types of OSI application protocols such as the X.500 protocol shown.

COMMENT 5

RCID during the communication monitors one type of used ITU standardized protocol.
That protocol itself incorporates the message (for instance a fax message)
See *FIG. fax communications ITU standard*

To comply with different types of OSI application protocols such as the X.500 protocol GREEN has to compulsively act on different (application) protocols.
Each protocol may "carry" one or more messages (for instance different types of office applications information)

With reference to **FIG. 2** and **FIG. 3b** the proxy 212 which is used to process communications complying with different types of OSI application protocols such as the X.500 protocol is NOT operational, nor has any direct influence on closing connections, at OSI level 1.

EXAMINER
...and
iv) a memory (see Fig.1, and col.7, lines 36-39 & 48-57), ...

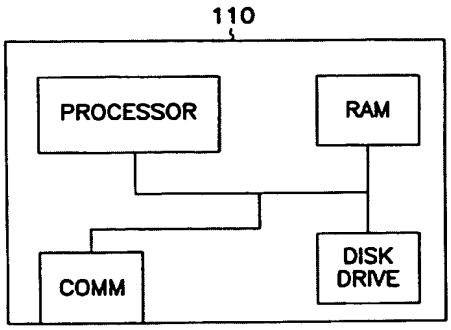


FIG. 1

GREEN col.7, lines 36-39
The current invention is an extension to the Sidewinder product. As shown in FIG. 1 generally at 110, a computer system comprises a processor 112 coupled to a random access memory, RAM 114.

GREEN col.7, lines 48-57
In FIG. 2, a computer program extension to the Sidewinder product is indicated generally at 210. The computer program is generally stored on the disk drive 120 and run or executed by the processor 112 out of RAM 114. It should be noted that disk drive 120 is used herein to represent various storage medium by which the computer program 210 may be stored and distributed. It also represents a communication medium in which the program may be temporarily stored while being transferred to computer system 110.

EXAMINER
...connected to the comparison and forwarding module, the memory unit storing characteristics of a standardized communications protocol of first communication device (see col.10, lines 40-43),...

GREEN col.10, lines 40-43
The filter maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error.

COMMENT 6
In general authentication is the process of identifying an individual or system, usually based on a user/system name and password. In security systems authentication is distinct from authorization, which is the process of giving individuals or systems access to system objects based on their identity.
Authentication merely ensures that the individual or system is who he or she claims to be, but says nothing about the access rights of the individual or system.

RCID does not use a filter which maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error.

RCID monitors the standardized ITU communication protocol.
In case of not allowed communication RCID always closes the communication in a standard way by PHISICALLY disconnecting both communication devices from each other.

GREEN is NOT developed to close disallowed communication by physically disconnecting at OSI level 1 with the result that simultaneously N+1 communication devices are disconnected.
GREEN **col.10, lines 40-43** speaks about a possible rejection.
That is very logical because physically closing down one connection means physically closing ALL allowed connections, so BRINGING DOWN THE ENTIRE CORPORATE NETWORK.

Additional GREEN makes the working of his invention useless because the firewall is not able to functioning anymore in case closing of the communication is performed at OSI level 1.

Persons of ordinary skill in the art will NEVER close communication in a physical way, because this will result in the same damaged as when a security incident occurs like a successful Denial of Service (DoS) attack initiated by a hacker.

GREEN **FIG. 3a** represents the level in the OSI model where the closing actions take place.
It is clear that closing actions are taking place in a LOGICAL way and not at OSI level 1.
That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated.

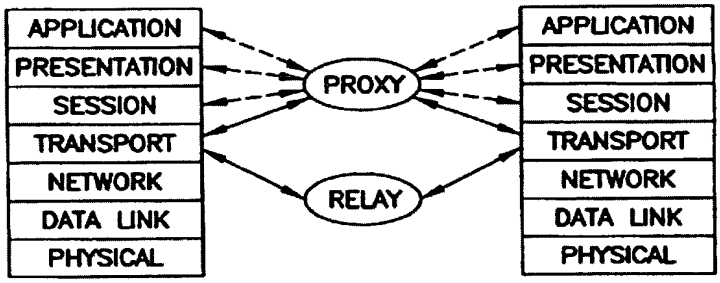


FIG. 3a

EXAMINER
...the comparison and forwarding module configured to compare the standardized communication protocol to a data protocol of incoming data from the first input (see col.5, lines 3-8; col.8, line 66 to col.9, line 5; and col.10, lines 40-43),...

GREEN col.5, lines 3-8
TCP proxies can be fitted with protocol specific filtering and appear "in-situ", with application data being examined and relayed in real time with only limited buffering, in contrast with the application gateway which would collect a full application context before relaying the data.

COMMENT 7
GREEN **FIG. 3a** represents the level in the OSI model where the closing actions take place.
It is clear that closing actions are taking place in a LOGICAL way and not at OSI level 1.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated.

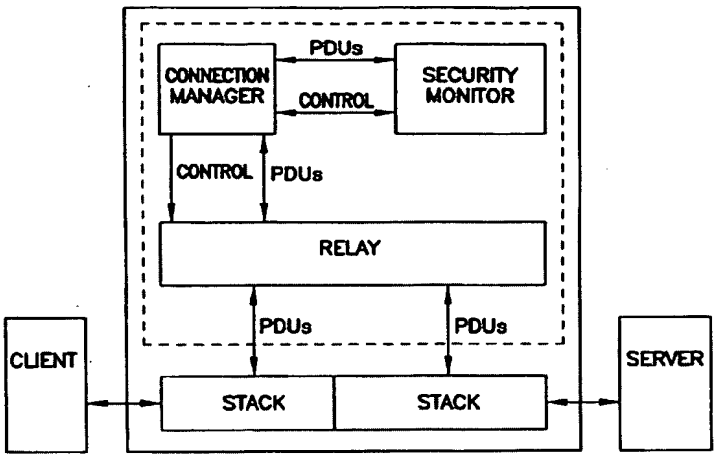


FIG. 3b

GREEN col.8, line 66 to col.9, line 5

Finally, to complete proxy processing and ensure that only specific OSI application data is being passed though the session, the proxy software continually examines the OSI application level protocols within the data frames. For example, in one embodiment, an X.500 proxy verifies that data exchanged during the session conforms to a specific X.500 protocol.

GREEN col.10, lines 40-43

The filter maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error.

COMMENT 8

See comment 6

EXAMINER

...and

i) to forward the incoming data to the second input when the comparison determines the data protocol conforms with the standardized communications protocol (see col.9, lines 41-43),...

GREEN col.9, lines 41-43

Once a connection is established between two devices on different networks, the proxy transparently forwards all X.500 PDUs (requests and their replies) to the two devices.

COMMENT 9

GREEN again points to the OSI levels where forwarding of data, so "closing or opening" of connections are taking place.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated.

EXAMINER

...and

ii) to physically open the communication link when the comparison determines the data protocol fails to conform with the standardized communication protocol (see col.10, lines 40-61; and col.12, lines 14-19);...

GREEN c I.10, lines 40-61

The filter maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error. The filter component then processes the BIND and returns status to the communications component. Based on the status, the proxy may pass the BIND on to the X.500 server, or it may cancel both sessions and close the connections. The status to be returned on error will be configurable. Because the proxy does not implement OSI transport, session, presentation, ACSE or ROSE layers, it will have to manually build appropriate responses to reject or even possibly abort a connection which may be in place. For example, if the proxy has an established TCP connection and a TP0 connection then receives a presentation P-- CONNECT request with an ACSE A-ASSOCIATE request for X.400 presentation context, the proxy must generate a rejection to this request, and close the connections. The proxy could be rude and just close the IP connection, but this is really not appropriate. The requester may just assume a network problem and retry the connection again. The appropriate response would be to build an ACSE A-ASSOCIATE response of "rejected (permanently)".

COMMENT 10

See comment 6
and
GREEN clearly confirms that closing a connection in a physical way is not appropriate. Quote *"...The proxy could be rude and just close the IP connection, but this is really not appropriate..."* unquote.
After all closing ONE connection physically means closing ALL logical connections.
As a result of closing the connection physically GREEN will be out of control during an amount of time.

RCID is always in control.

GREEN col.12, lines 14-19

5. The network communication session manager of claim 2 wherein the plurality of distinct layers includes a presentation layer, a session layer and a transport layer and wherein the connection manager rejects a remote responding entity by generating a response at the presentation layer, the session layer, and the transport layer.

COMMENT 11

GREEN **col.12, lines 14-19** clearly describes the upper OSI layers where "closing" actions are taking place.
That is very logical because physically closing ONE connection means closing ALL dependent logical connections, so BRINGING DOWN THE ENTIRE CORPORATE NETWORK.

Additional GREEN makes the working of his invention useless because the firewall is not able to functioning anymore in case the above procedure is executed.

GREEN **FIG. 3a** represents the level in the OSI model where the closing actions take place.
It is clear that closing actions are taking place in a LOGICAL way.

Closing a connection in a physical way is only possible in OSI layer 1.
All the above layers are after all dependent of OSI layer 1.

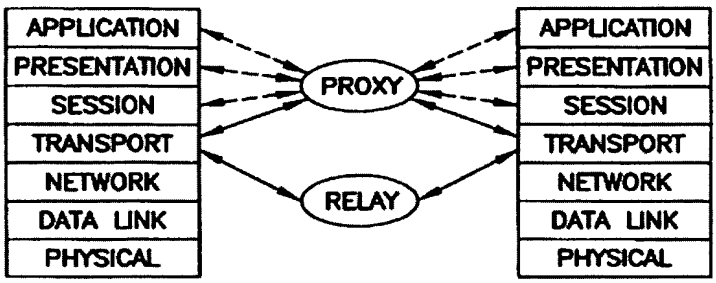


FIG. 3a

EXAMINER
(ii) comparing the data protocol of the data with the standardized communication protocol in the data communication protection device (10) (see col.8, line 66 to col.9, line 5),...

GREEN col.8, line 66 to col.9, line 5
Finally, to complete proxy processing and ensure that only specific OSI application data is being passed though the session, the proxy software continually examines the OSI application level protocols within the data frames. For example, in one embodiment, an X.500 proxy verifies that data exchanged during the session conforms to a specific X.500 protocol.

COMMENT 12
GREEN **col.12, lines 14-19** clearly describes the upper OSI layers where examination is done and actions e.g. "closing" connections are taking place.
That is very logical because physically closing ONE connection means closing ALL dependent logical connections, so BRINGING DOWN THE ENTIRE CORPORATE NETWORK.

Additional GREEN makes the working of his invention useless because the firewall is not able to functioning anymore in case the above procedure is executed.

GREEN **FIG. 3a** represents the level in the OSI model where the closing actions take place.
It is clear that closing actions are taking place in a LOGICAL way.

Closing a connection in a physical way is only possible in OSI layer 1.
All the above layers are after all dependent of OSI layer 1.

EXAMINER
...characterized by
(iii) forwarding data of which the data protocol complies with the standardized communication protocol from the data communication protection device (10) to the first communication station (11) (see col.9, lines 41-43),...

GREEN col.9, lines 41-43
Once a connection is established between two devices on different networks, the proxy transparently forwards all X.500 PDUs (requests and their replies) to the two devices.

COMMENT 13
See comment 12

EXAMINER
...and not forwarding data of which the data protocol does not comply with the standardized communication protocol from the data communication protection device to the first communication station (see col.10, lines 40-43, lines 48-57, & lines 60-61; and col.12, lines 14-19)...

GREEN col.10, lines 40-43
The filter maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error.

COMMENT 14
This part refers to the way user identification and user authorization is being handled.
Depending on the results a rejection should be returned on error.
The configuration file must always be up-to-date.

RCID only monitors if the used protocol conforms the ITU standardized protocol.
There is no configuration file which must be up-to-date what so ever.
The only possible rejection on error is closing the physical connection.

GREEN col.10, lines 48-57
Because the proxy does not implement OSI transport, session, presentation, ACSE or ROSE layers, it will have to manually build appropriate responses to reject or even possibly abort a connection which may be in place. For example, if the proxy has an established TCP connection and a TP0 connection then receives a presentation P-- CONNECT request with an ACSE A-ASSOCIATE request for X.400 presentation context, the proxy must generate a rejection to this request, and close the connections.

COMMENT 15
GREEN **col.10, lines 48-57** clearly describes the upper OSI layers where "closing" actions are taking place.

That is very logical because physically closing ONE connection means closing ALL dependent logical connections, so BRINGING DOWN THE ENTIRE CORPORATE NETWORK.

Additional GREEN makes the working of his invention useless because the firewall is not able to functioning anymore in case the above procedure is executed.

RCID does not have to manually build appropriate responses to reject or even possibly abort a connection which may be in place.
RCID only knows one action: Close the connection physically.

GREEN col.10, lines 60-61
The appropriate response would be to build an ACSE A-ASSOCIATE response of "rejected (permanently)".

COMMENT 16
See comment 15

GREEN col.12, lines 14-19
5. The network communication session manager of claim 2 wherein the plurality of distinct layers includes a presentation layer, a session layer and a transport layer and wherein the connection manager rejects a remote responding entity by generating a response at the presentation layer, the session layer, and the transport layer.

COMMENT 17
Closing a connection in a physical way is only possible at OSI layer 1.
All the above layers are after all dependent of OSI layer 1.

GREEN clearly describes the upper OSI layers where examination is done and actions e.g. "closing" connections (forwarding) are taking place.
With great emphasis GREEN excludes the use of OSI layer 1 as a way to close connections.
That is very logical because physically closing ONE physical connection means closing ALL dependent logical connections, so BRINGING DOWN THE ENTIRE CORPORATE NETWORK.

Additional GREEN makes the working of his invention useless because the firewall is not able to functioning anymore in case the above procedure is executed.

GREEN **FIG. 3a** represents the level in the OSI model where the closing actions take place.
It is clear that closing actions are taking place in a LOGICAL way.

With great emphasis GREEN **FIG. 2**, **FIG. 3a**, **FIG. 3b** and **FIG. 4** exclude the use of OSI layer 1 as a way to close a logical connection.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated indeed.

RCID **always** close a connection at OSI layer 1.

GREEN **never** closes a connection at OSI layer 1.

EXAMINER
...by physically opening the communication link within the protection device to prevent communications between the first communication station (11) and the second communication station (12) (see col.10, lines 43-47, 51, and 56-57).

GREEN col.10, lines 43-47
The filter component then processes the BIND and returns status to the communications component. Based on the status, the proxy may pass the BIND on to the X.500 server, or it may cancel both sessions and close the connections.

COMMENT 18
See comment 17

GREEN col.10, line 51
...possibly abort a connection which may be in place. For...

COMMENT 19
See comment 17

GREEN col.10, lines 56-57
...generate a rejection to this request, and close the connections. The proxy could be rude and just close the IP, but this is really not appropriate.

COMMENT 20
See comment 17

EXAMINER
It is inherent that when communication links are physically opened the communication links can no longer transfer current thereby preventing data to be communicated and therefore does not patentably distinguish the invention.

As per claim 4, Green teaches of a data communication protection device (10) (see Fig.1 and col.7, lines 36-47)...

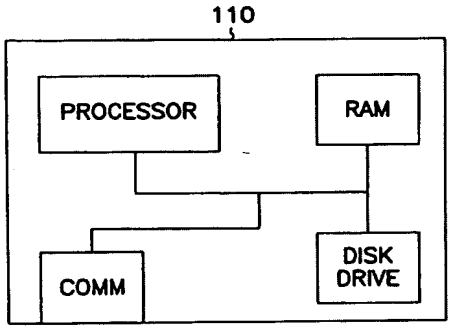


FIG. 1

GREEN col.7, lines 36-47
The current invention is an extension to the Sidewinder product. As shown in FIG. 1 generally at 110, a computer system comprises a processor 112 coupled to a random access memory, RAM 114. While only a single bus 116 is shown connecting the RAM 114 and processor 112 to a communications port 118 and disk drive or other storage medium 120, it will be recognized by those skilled in the art that it represents several different busses in a standard personal computer architecture. The communications port represents various communications options in computer systems, such as ethernet cards, modems and other communication devices.

COMMENT 21
See comment 17
And
Also in a WIRELESS environment the state of affairs for GREEN and RCID will stay the same as described in comment 17.

EXAMINER
...arranged for protecting data communication traffic between a first communication station (11) (see Fig.2, #216; and col.7, lines 60-62) and a second communication station (12) (see Fig.2, #214; and col.7, lines 60-62),...

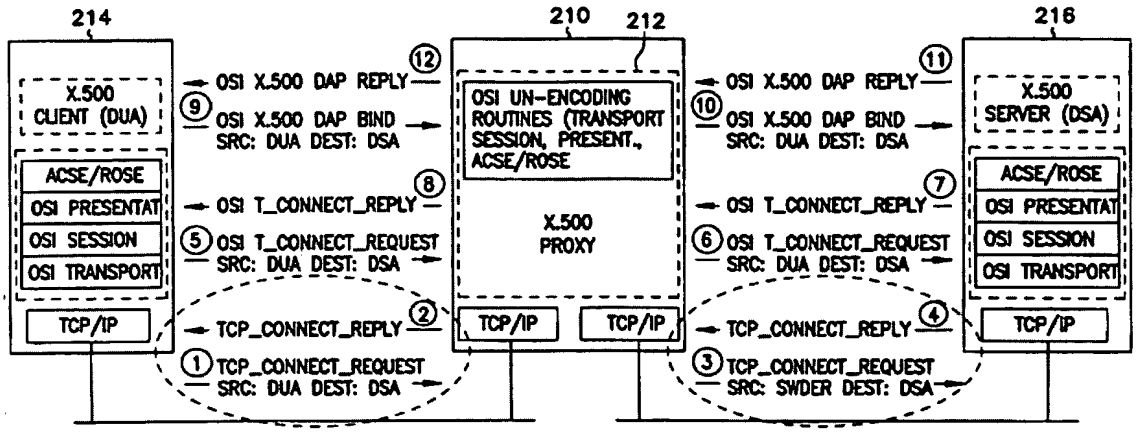


FIG. 2

GREEN col.7, lines 60-62
Also shown in FIG. 2 are a client 214 and server 216 for which connections and data transfers will be described further below.

COMMENT 22
With great emphasis GREEN FIG. 2 excludes the use of OSI layer 1 as a way to close a logical connection.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated indeed.

EXAMINER
...data being dispatched according to a data protocol from the second communication station to the first communication station (see col.5, lines 29-32),...

GREEN col.5, lines 29-32
Protocol data units are interrogated for conformance to a protocol session, and optionally further decoded to add additional application specific filtering.

EXAMINER
...the data communication protection device comprising: a first input for connection to an incoming communication line receiving the data communication from the second communication station (see Fig.2, and Fig.3b); a second input for connection to the first communication station (see Fig.2, and Fig.3b);...

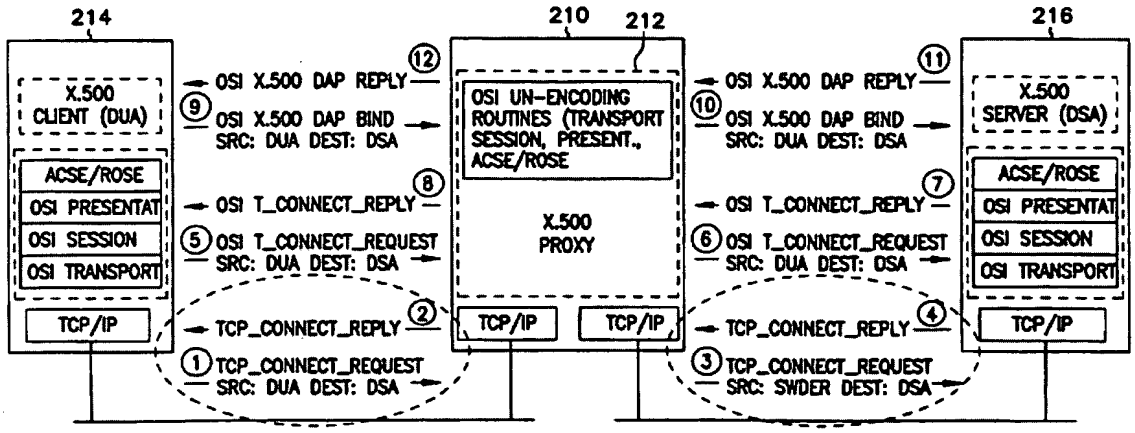


FIG. 2

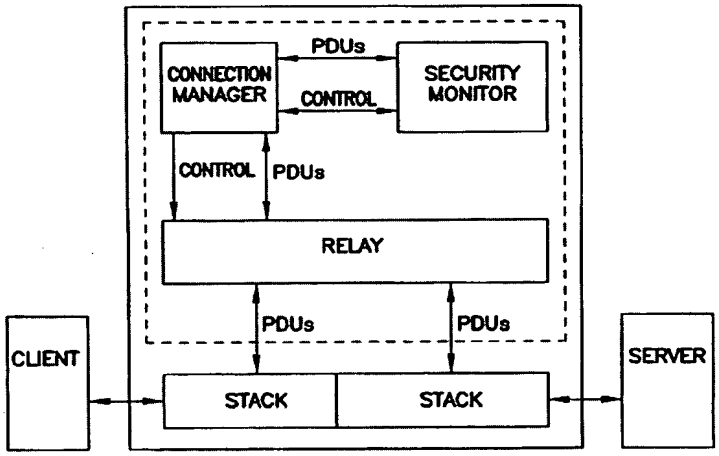


FIG. 3b

COMMENT 23

With great emphasis both GREEN FIG. 2 and GREEN FIG. 3b excludes the use of OSI layer 1 as a way to close a logical connection.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated indeed.

EXAMINER

...a comparison and forwarding module connected intermediate the first input and the second input and establishing a physical communication link between the first input and the second input (see Fig.2, #212 and col.7, lines 57-60);...

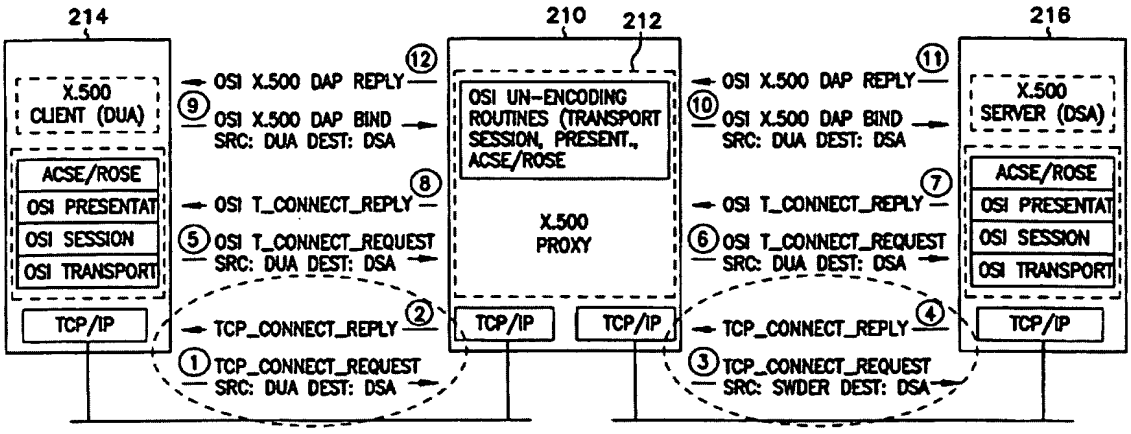


FIG. 2

COMMENT 24

With great emphasis GREEN **FIG. 2** excludes the use of OSI layer 1 as a way to close a logical connection.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated indeed.

GREEN col.7, lines 57-69

Computer program 210 further comprises a proxy 212 which is used to process communications complying with different types of OSI application protocols such as the X.500 protocol shown. Also shown in FIG. 2 are a client 214 and server 216 for which connections and data transfers will be described further below. The Sidewinder security system has special TCP/IP networking modifications which allow it to accept a TCP connection request even though the data was not addressed to it. The Sidewinder can then verify the data and establish another independent session with the real destination device using the destination address specified within the senders original request.

COMMENT 25

Quote *"...and establish another independent session with..."* unquote.

GREEN describes the setup of a LOGICAL communication path in case a request is approved. It goes without saying that such build connection is closed in a logical way to.

With great emphasis GREEN **col.7, lines 57-69** exclude the use of OSI layer 1 as a way to close a logical connection.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated indeed.

EXAMINER

...and a memory (see Fig.1, and col.7, lines 36-39 & 48-57)...

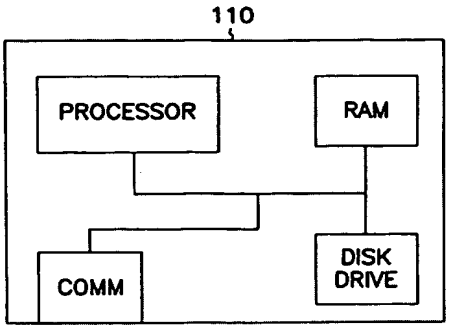


FIG. 1

GREEN col.7, lines 36-39

The current invention is an extension to the Sidewinder product. As shown in FIG. 1 generally at 110, a computer system comprises a processor 112 coupled to a random access memory, RAM 114.

GREEN col.7, lines 48-57

In FIG. 2, a computer program extension to the Sidewinder product is indicated generally at 210. The computer program is generally stored on the disk drive 120 and run or executed by the processor 112 out of RAM 114. It should be noted that disk drive 120 is used herein to represent various storage medium by which the computer program 210 may be stored and distributed. It also represents a communication medium in which the program may be temporarily stored while being transferred to computer system 110.

EXAMINER

...connected to the comparison and forwarding module, the memory unit storing characteristics of a standardized communication protocol of first communication device (see col.10, lines 40-43), the comparison and forwarding module configured to compare the standardized communication protocol to a data protocol of incoming data from the first input (see col.5, lines 3-8; col.8, line 66 to col.9, line 5; and col.10, lines 40-43), and...

GREEN col.10, lines 40-43

The filter maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error.

COMMENT 26

RCID does not use a filter which maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error.

RCID monitors the standardized ITU communication protocol.

GREEN col.5, lines 3-8

TCP proxies can be fitted with protocol specific filtering and appear "in-situ", with application data being examined and relayed in real time with only limited buffering, in contrast with the application gateway which would collect a full application context before relaying the data.

COMMENT 27

RCID does not use a filter which maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error.

RCID monitors the standardized ITU communication protocol.

GREEN col.8, lin 66 to c l.9, line 5

Finally, to complete proxy processing and ensure that only specific OSI application data is being passed though the session, the proxy software continually examines the OSI application level protocols within the data frames. For example, in one embodiment, an X.500 proxy verifies that data exchanged during the session conforms to a specific X.500 protocol.

COMMENT 28

GREEN again points to the OSI levels where forwarding of data, so "closing or opening" of connections are taking place.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated.

GREEN col.10, lines 40-43

The filter maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error.

COMMENT 29

RCID does not use a filter which maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error.
RCID monitors the standardized ITU communication protocol.

EXAMINER

i) to forward the incoming data to the second input when the comparison determines the data protocol conforms with the standardized communications protocol (see col.9, lines 41-43)...

GREEN col.9, lines 41-43

Once a connection is established between two devices on different networks, the proxy transparently forwards all X.500 PDUs (requests and their replies) to the two devices.

COMMENT 30

GREEN again points to the OSI levels where forwarding of data, so "closing or opening" of connections are taking place.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated.

EXAMINER

...and
ii) to physically open the communication link when the comparison determines the data protocol fails to conform with the standardized communication protocol (see col.10, lines 40-61; and col.12, lines 14-19).

GREEN col.10, lines 40-61

The filter maintains a configuration file containing what type of authentication is allowed, who is allowed, and what possible rejection should be returned on error. The filter component then processes the BIND and returns status to the communications component. Based on the status, the proxy may pass the BIND on to the X.500 server, or it may cancel both sessions and close the connections. The status to be returned on error will be configurable. Because the proxy does not implement OSI transport, session, presentation, ACSE or ROSE layers, it will have to manually build appropriate responses to reject or even possibly abort a connection which may be in place. For example, if the proxy has an established TCP connection and a TP0 connection then receives a presentation P-- CONNECT request with an ACSE A-ASSOCIATE request for X.400 presentation context, the proxy must generate a rejection to this request, and close the

connections. The proxy could be rude and just close the IP connection, but this is really not appropriate. The requester may just assume a network problem and retry the connection again. The appropriate response would be to build an ACSE A-ASSOCIATE response of "rejected (permanently)".

COMMENT 31

See comment 6
and
GREEN clearly confirms that closing a connection in a physical way is not appropriate. Quote *"...The proxy could be rude and just close the IP connection, but this is really not appropriate..."* unquote.
After all closing ONE connection physically means closing ALL logical connections.
As a result of closing the connection physically GREEN will be out of control during an amount of time.

RCID is always in control.

GREEN col.12, lines 14-19

5. The network communication session manager of claim 2 wherein the plurality of distinct layers includes a presentation layer, a session layer and a transport layer and wherein the connection manager rejects a remote responding entity by generating a response at the presentation layer, the session layer, and the transport layer.

COMMENT 32

GREEN **col.12, lines 14-19** clearly describes the upper OSI layers where "closing" actions are taking place.

That is very logical because physically closing ONE connection means closing ALL dependent logical connections, so BRINGING DOWN THE ENTIRE CORPORATE NETWORK.

Additional GREEN makes the working of his invention useless because the firewall is not able to functioning anymore in case the above procedure is executed.

RCID does not have to manually build appropriate responses to reject or even possibly abort a connection which may be in place.
RCID only knows one action: Close the connection physically.

EXAMINER

As per claims 20, Green further teaches wherein the standardized communication protocol is other than a TCP/IP protocol component (see col. 11, lines 44-47).

GREEN col.11, lines 44-47

In addition, further communication protocols may also be used, and the claims should not be limited to those that have been described.

EXAMINER

As per claims 11, 13, 15, 17, and 19, Green further teaches wherein when the comparison and forwarding module opens the communication link, a data file of the incoming data is stored in the memory (see col.4, lines 31-33 & 48-61 and col.5, line 6).

GREEN col.4, lines 31-33

The firewall may have to buffer large amounts of data before being able to relay the data to the other independent application association.

GREEN c I.4, lines 48-61

If a proxy were to operate at a data link layer, referred to as a MAC layer, it would capture Ethernet frames and examine the addresses in the MAC header, and filter the payload portion (IP datagrams) to determine Internet Protocol IP addresses. Higher layer filtering would be infeasible because data would have to be buffered and reassembled in order to gain enough context, and the semantics of TCP are such that only limited number of frames could be buffered and examined before it would become necessary to send them in order to receive more. So if only a partial security context has been determined when the buffer threshold was reached, the data would have to either be discarded or sent without full validation-in either case, an unacceptable alternative for OSI application.

GREEN col.5, line 6

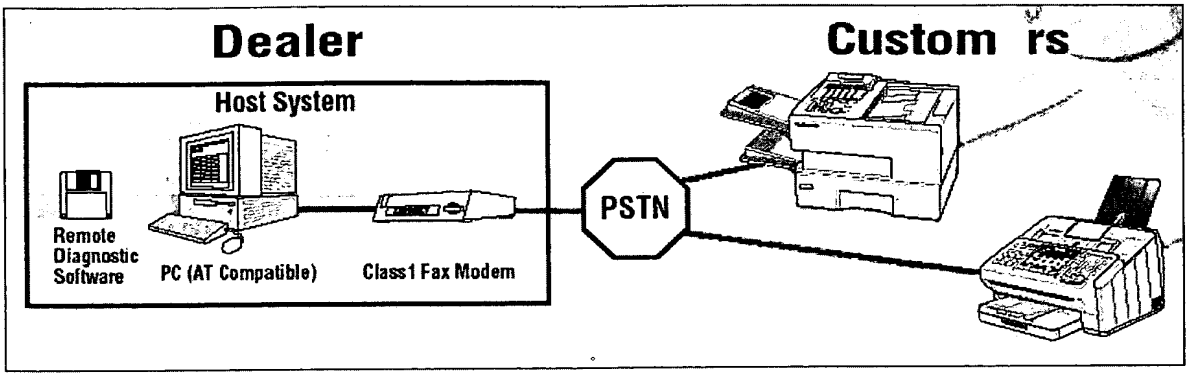
...time with only limited buffering, in contrast with the application...

COMMENT 33

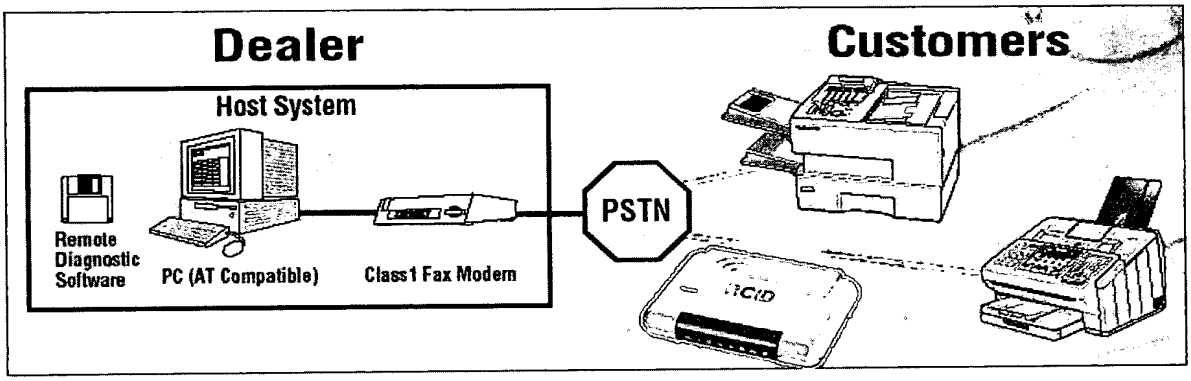
GREEN again points to the OSI levels where forwarding of data, so "closing or opening" of connections are taking place.

That makes sense because the firewall is not able to functioning anymore in case communication at OSI level 1 is terminated.

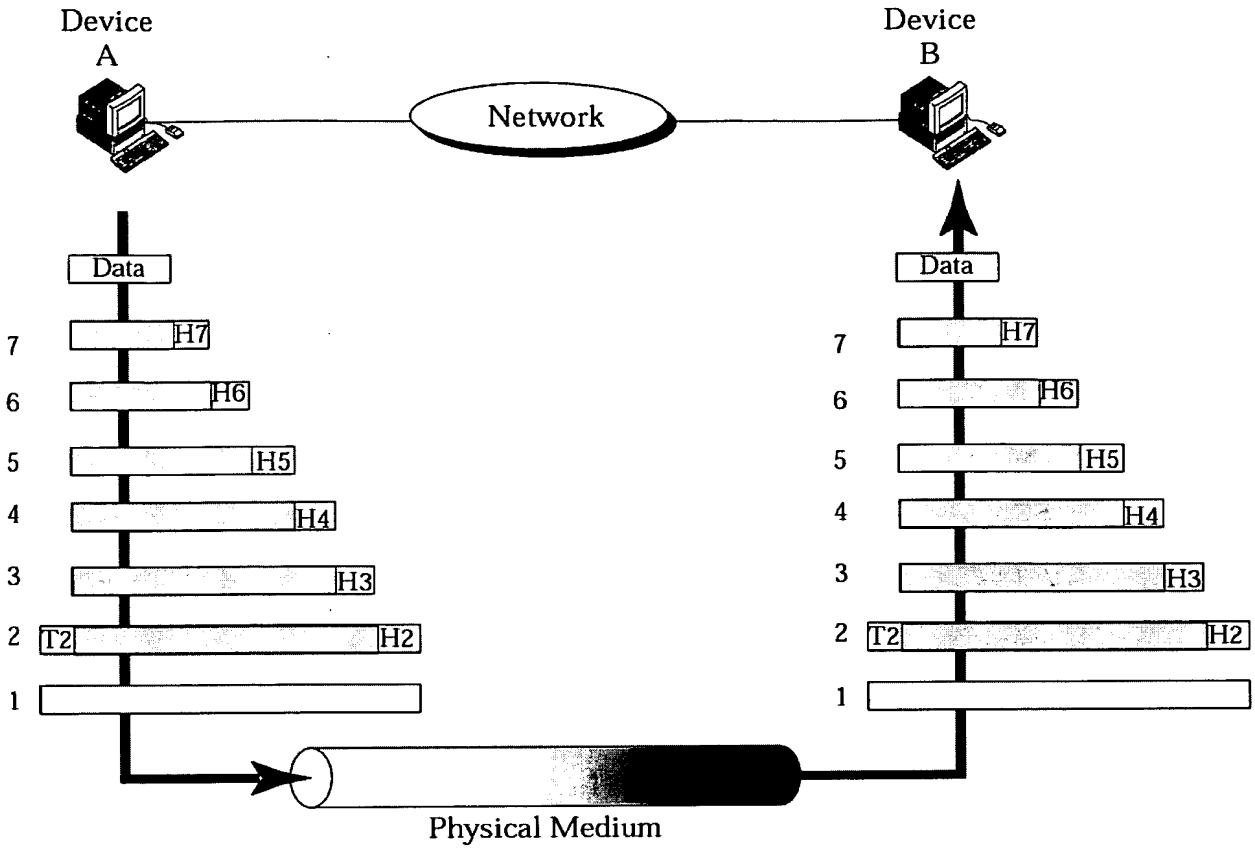
Abus of Rem t Diagn stics



Unprotected fax machines...



With RCID protected fax machines...



RCID

- In the above presented picture device A and device B both represent <u>one</u> device indeed.
- RCID connects and disconnects at OSI level 1.
- Disconnecting at OSI level 1 is the goal of RCID.
- Disconnecting at OSI level 1 will result in a save and desired state which will prevent the loss of property (files, proprietary information, etc.)

GREEN

- In the above presented picture device A and device B both represent <u>N+1</u> devices.
- GREEN "connects" and "disconnects" (setting up sessions) <u>not</u> at OSI level 1.
- Disconnecting different from OSI level 1 is the goal of GREEN.
- Disconnecting at OSI level 1 will immediately result in bringing down the complete corporate network which will lead to loss of property (files, proprietary information, etc.)

RCID	Gr en
Protection DEVICE vs prot ction Application(s)	
Controls the connection to the **device**. • *It is to the full advantage of the protected device when during a security event the connection will be broken physically.*	Controls the connection to one or more **applications** • *It is to the full advantage of the specific protected application when during a security event the connection will be broken logically.* • *Breaking the connection physically will inevitable lead to a break down of ALL approved connections.* ***Thus creating an information security incident by Green itself.*** See for instance fig 2 / fig3a / fig 3b /fig 4 Col 5 sentence 17
Judgement	
Evaluates the protocol as a **whole**.	Evaluates only the **P**rotocol **D**ata **U**nits (**PDU**) of which rules are given in the access control list. See for instance Fig 3b Col 8 sentence 15-17
Range of kind of protocol	
Does **NOT** limit the protection with respect to protocols based on the TCP-IP layer.	**LIMITS** the protection with respect to protocols based on the TCP-IP layer alone. See for instance Col 8 sentence 15-17 Col 9 sentence 66-Col 10 sentence 3 Col 11 sentence 1-2 Col 12 sentence 32-36 Col 14 sentence 61-64
Guards on th basis of	

Evaluates if a protocol is an approved <u>international standard</u>.	Evaluates the Protocol Data Units (PDU) of which rules are given in the <u>access control list</u>.
• *The system administrator does not need to configure the RCID device.*	• *For the proper working of Green, the system administrator needs to configure the Access Control List (ACL) and keep that ACL up to date.*
• *The device to protect is **<u>ALLWAYS</u>** safeguarded by RCID.*	• *The applications to protect are **<u>NOT</u>** always safeguarded by Green eg when the ACL is not configured, not complete or not up to date.*
• *RCID can be installed "out of the box".*	• *Green can **<u>not</u>** be installed "out of the box" and demands that a mandatory Access Control List must be configured.* See for instance Col 5 sentence 22, 27, 39-45 Col 10 sentence 9-12 Col 13 sentence 7, 47

Disconn ction of the connection	
When a security event occurs, the connection will be broken **PHYSICALLY ALLWAYS**	When a security event occurs, the connection will be broken **LOGICALLY ALLWAYS**
• *This **IS inherent** to the design of RCID.*	• *This **is NOT inherent** to the intention and design of Green.*
• *It is inevitable **that NO communication is possible at all** when the connection is PHYSICALLY broken.*	• *It is inevitable **that NO communication is possible at all** when the connection is PHYSICALLY broken. eg **all approved connections also will be terminated**.*
• *The special design of RCID provides the **optimum protection** when terminating the connection in a physical way.*	• *Because of the design of Green, Green is **not able to function** as intended when the connection will be physically broken.*
• *It is emphasized that the working of RCID **enforces** to break the connection physically at **all** times a security breach occurs.*	• *It is emphasized that the working of Green **enforces** to break the connection logically at **all** times a security breach occurs.*
• *In the event of a security breach no connection is necessary at all.*	• *In the event of a security breach no connection is necessary for **that specific** application*
	• *At the moment Green breaks the connection physically **the network will be down completely**.*
	• *If the network goes down completely Green is the **cause of a major information security incident** itself. (the integrity of data and the availability of data and the mend network)*
	See for instance Fig 3a / 3b Col 5 sentence 24-26, 39-45 Col 6 sentence 17-20 Col 8 sentence 17-25 Col 10 sentence 57, 60

	Col 12 sentence 8, 17-20, 39-44
Relation	
There is an one on one (1 on 1) relation Device ➔ RCID ➔ Device There is no hierarchy at all.	There is an one on "n" (1 on n) relation Device ➔ Green ➔ Devices There is hierarchy present. (one server and one or more clients) See for instance fig 2 / fig3a / fig 3b /fig 4 Col 1 sentence 5-7